Partial English Translation of

LAID OPEN unexamined

JAPANESE PATENT APPLICATION

Publication No. 2001-024876

[0072] to [0073]

[0072] Next, a case where "VC" is to be replaced thereby will be considered (Method 2).

[0073] Herein, the effective coefficient is expressed by the smallest bit number, as described above. Hence, no zero run length is involved as in the case of "VC". Regarding the code replacement, any method can be employed if the bit number does not change. The reason for this is that no change occurs in the group number in the change in which no change occurs in the bit number, whereby appropriate decoding is enabled. Regarding the actual replacement, it can be considered to replace the bit at a place where the code in question is positioned by the bit of an embedded raw image. Herein, the bit position can be selected according to the random number.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-024876
(43)Date of publication of application : 26.01.2001

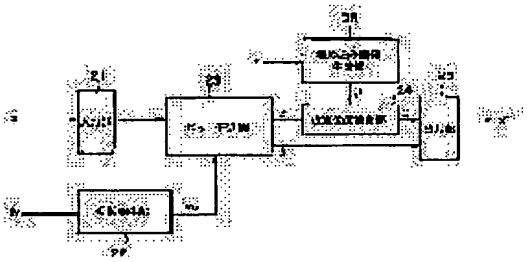
(51)Int.Cl. H04N 1/387
G06F 12/14
G06T 1/00

(21)Application number : 11-193332
(22)Date of filing : 07.07.1999

(71)Applicant : CANON INC
(72)Inventor : HAYASHI JUNICHI
WAKAO SATOSHI

(54) METHOD AND DEVICE FOR IMAGE PROCESSING AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To detect an alteration position when the alteration is performed by inputting image position information for instructing an image position at which another data are embedded in image data, generating sub-key information at a random number based on main key information and changing pixel data of the image position of the image data decided based on the image position information based on the sub-key information.
SOLUTION: In an extracting device of an electronic watermark, data to be inputted to an input part 21 are embedded image data (x') of the electronic watermark outputted from an electronic watermark embedding device and are inputted to a bit extractor 23. Also, a random number initial value Iv to be inputted to a random number generation part 22 is an initial value to the random number generation part 22, that is, main key information. The random number generator 22 to which the random number initial value Iv (the main key information) is inputted generates a random number progression (sub-key information) Rn and the generated random number progression Rn is inputted to the bit extractor 23. In the bit extractor 23, bit information is extracted from the embedded image data (x') by using this random number progression Rn.



LEGAL STATUS

[Date of request for examination] 06.10.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－24876
（P2001－24876A）
(43)公開日　平成13年１月26日(2001.1.26)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｂ０５７
Ｇ０６Ｔ　1/00		15/66	Ｂ	５Ｃ０７６

審査請求　未請求　請求項の数26　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－193332

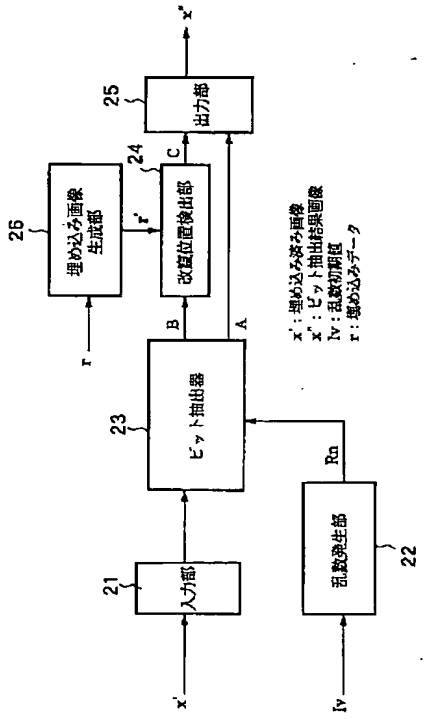
(22)出願日　平成11年７月７日(1999.7.7)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　林　淳一
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(72)発明者　若尾　聡
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100076428
弁理士　大塚　康徳　（外２名）

最終頁に続く

(54)【発明の名称】　画像処理方法及び装置と記憶媒体

(57)【要約】
【課題】　データに対して人為的な改竄がなされた場合に、その改竄位置を確実に検出する。
【解決手段】　画像データに別のデータを埋め込む画像位置を指示する埋め込みデータｒを入力し、その埋め込みデータｒに基づいて決定される画像データの画素データを、主鍵情報Ｉｖに基づいて乱数的に生成された副鍵情報Ｒｎに基づいて変更した埋め込み済み画像データｘ’を生成する。この埋め込み済み画像データｘ’を入力し、主鍵情報Ｉｖに基づいて乱数的に生成された副鍵情報Ｒｎに基づいて、そのデータｘ’からビット情報を抽出し、そのビット情報の位置が埋め込みデータｒによって指示された位置に等しいかどうかによって、その埋め込み済み画像データｘ’の改竄された位置を知ることができる。



1

【特許請求の範囲】

【請求項１】　画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力手段と、
主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成手段と、
前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更手段と、を有することを特徴とする画像処理装置。

【請求項２】　画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力手段と、
前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成手段と、
前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出手段と、
前記抽出手段により抽出された前記画素データと前記鍵情報生成手段により生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較手段とを有し、
前記比較手段による比較結果に応じて前記埋め込み済み画像データの改竄位置を検出することを特徴とする画像処理装置。

【請求項３】　前記画像データは多値画像データであって、前記副鍵情報は前記多値画像データの画素データのビット位置を指示する情報であることを特徴とする請求項１又は２に記載の画像処理装置。

【請求項４】　前記画像データは符号化データであり、
前記符号化データを解析する解析手段と、
前記解析手段による解析に基づいて前記符号化データの符号を置き換える置換手段と、を更に有することを特徴とする請求項１に記載の画像処理装置。

【請求項５】　前記符号化データが、入力系列において非零の係数から次の非零の係数までの係数の個数と、前記次の非零の係数の値の組合せをハフマン符号化した符号化データである場合、
前記置換手段は、前記非零の係数から次の係数までの係数の個数に対応するハフマン符号を前記非零の係数から前記次の非零の係数までの個数が変化しないように置き換えることを特徴とする請求項４に記載の画像処理装置。

【請求項６】　前記符号化データが、入力系列において非零の係数から次の非零の係数までの係数の個数と、前記次の非零の係数の値の組合せをハフマン符号化した符号化データである場合、
前記置換手段は、前記次の係数の値に対応するハフマン符号を置き換えることを特徴とする請求項４に記載の画像処理装置。

2

【請求項７】　前記別のデータが電子透かしを含むことを特徴とする請求項１に記載の画像処理装置。

【請求項８】　埋め込みデータに従って入力画像データの位置を特定する位置特定手段と、
主鍵情報から副鍵情報を乱数的に生成する鍵情報生成手段と、
前記位置特定手段により特定された位置の画素情報を前記副鍵情報に基づいて別のデータに置き換える置換手段と、
前記置換手段により前記別のデータに置き換えられたデータに対して演算を行う演算手段と、
前記別のデータに置き換えられたデータと前記演算手段による演算結果とを合成して出力する合成手段と、を有することを特徴とする画像処理装置。

【請求項９】　埋め込みデータに従って入力画像データの位置を特定された位置の画素情報を、主鍵情報から乱数的に生成された副鍵情報に基づいて別のデータに置き換え、前記別のデータに置き換えられたデータに対して実行された演算の結果とを合成して得られたデータを入力する入力手段と、
前記入力手段により入力されたデータを解析して前記データと前記演算の結果を抽出する解析手段と、
前記解析手段により抽出された前記データを演算する演算手段と、
前記解析手段により抽出された前記演算の結果と前記演算手段による演算結果とを比較する比較手段と、を有することを特徴とする画像処理装置。

【請求項１０】　前記入力画像データは符号化データであり、
前記符号化データを解析する解析手段と、
前記符号化データの符号の位置を乱数的に選択し、前記選択された符号の位置のビットを抽出する手段を更に有することを特徴とする請求項８に記載の画像処理装置。

【請求項１１】　前記演算手段による演算はハッシュ値を算出する演算であることを特徴とする請求項８又は９に記載の画像処理装置。

【請求項１２】　画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力工程と、
主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成工程と、
前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更工程と、を有することを特徴とする画像処理方法。

【請求項１３】　画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力工程と、

前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成工程と、
前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出工程と、
前記抽出工程で抽出された前記画素データと前記鍵情報生成工程で生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較工程とを有し、
前記比較工程による比較結果に応じて前記埋め込み済み画像データの改竄位置を検出することを特徴とする画像処理方法。

【請求項１４】　前記画像データは多値画像データであって、前記副鍵情報は前記多値画像データの画素データのビット位置を指示する情報であることを特徴とする請求項１２又は１３に記載の画像処理方法。

【請求項１５】　前記画像データは符号化データであり、前記符号化データを解析する解析工程と、
前記解析工程における解析に基づいて前記符号化データの符号を置き換える置換工程と、を更に有することを特徴とする請求項１２に記載の画像処理方法。

【請求項１６】　前記符号化データが、入力系列において非零の係数から次の非零の係数までの係数の個数と、前記次の非零の係数の値の組合せをハフマン符号化した符号化データである場合、
前記置換工程では、前記非零の係数から次の係数までの係数の個数に対応するハフマン符号を前記非零の係数から前記次の非零の係数までの個数が変化しないように置き換えることを特徴とする請求項１５に記載の画像処理方法。

【請求項１７】　前記符号化データが、入力系列において非零の係数から次の非零の係数までの係数の個数と、前記次の非零の係数の値の組合せをハフマン符号化した符号化データである場合、
前記置換工程では、前記次の係数の値に対応するハフマン符号を置き換えることを特徴とする請求項１５に記載の画像処理方法。

【請求項１８】　前記別のデータが電子透かしを含むことを特徴とする請求項１２に記載の画像処理方法。

【請求項１９】　埋め込みデータに従って入力画像データの位置を特定する位置特定工程と、
主鍵情報から副鍵情報を乱数的に生成する鍵情報生成工程と、
前記位置特定工程で特定された位置の画素情報を前記副鍵情報に基づいて別のデータに置き換える置換工程と、
前記置換工程で前記別のデータに置き換えられたデータに対して演算を行う演算工程と、
前記別のデータに置き換えられたデータと前記演算手段による演算結果とを合成して出力する合成工程と、を有することを特徴とする画像処理方法。

【請求項２０】　埋め込みデータに従って入力画像データの位置を特定された位置の画素情報を、主鍵情報から乱数的に生成された副鍵情報に基づいて別のデータに置き換え、前記別のデータに置き換えられたデータに対して実行された演算の結果とを合成して得られたデータを入力する入力工程と、
前記入力工程で入力されたデータを解析して前記データと前記演算の結果を抽出する解析工程と、
前記解析工程で抽出された前記データを演算する演算工程と、
前記解析工程で抽出された前記演算の結果と前記演算工程による演算結果とを比較する比較工程と、を有することを特徴とする画像処理方法。

【請求項２１】　前記入力画像データは符号化データであり、
前記符号化データを解析する解析工程と、
前記符号化データの符号の位置を乱数的に選択し、前記選択された符号の位置のビットを抽出する工程を更に有することを特徴とする請求項１９に記載の画像処理方法。

【請求項２２】　前記演算工程における演算はハッシュ値を算出する演算であることを特徴とする請求項１９又は２０に記載の画像処理方法。

【請求項２３】　コンピュータにより読取り可能な記憶媒体であって、
画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力工程モジュールと、
主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成工程モジュールと、
前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更工程モジュールと、を有することを特徴とする記憶媒体。

【請求項２４】　画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力工程モジュールと、
前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成工程モジュールと、
前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出工程モジュールと、
前記抽出工程で抽出された前記画素データと前記鍵情報生成工程で生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較工程モジュールとを有することを特徴とする記憶媒体。

【請求項２５】　埋め込みデータに従って入力画像データの位置を特定する位置特定工程モジュールと、
主鍵情報から副鍵情報を乱数的に生成する鍵情報生成工程モジュールと、
前記位置特定工程で特定された位置の画素情報を前記副

鍵情報に基づいて別のデータに置き換える置換工程モジュールと、
前記置換工程で前記別のデータに置き換えられたデータに対して演算を行う演算工程モジュールと、
前記別のデータに置き換えられたデータと前記演算手段による演算結果とを合成して出力する合成工程モジュールと、を有することを特徴とする記憶媒体。
【請求項２６】　埋め込みデータに従って入力画像データの位置を特定された位置の画素情報を、主鍵情報から乱数的に生成された副鍵情報に基づいて別のデータに置き換え、前記別のデータに置き換えられたデータに対して実行された演算の結果とを合成して得られたデータを入力する入力工程モジュールと、
前記入力工程で入力されたデータを解析して前記データと前記演算の結果を抽出する解析工程モジュールと、
前記解析工程で抽出された前記データを演算する演算工程モジュールと、
前記解析工程で抽出された前記演算の結果と前記演算工程による演算結果とを比較する比較工程モジュールと、を有することを特徴とする記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、原画像データに電子透かしを埋め込んだ画像データを生成し、及び或はその画像データの改竄された箇所を特定する画像処理方法及び装置と記憶媒体に関するものである。
【０００２】
【従来の技術】近年のコンピュータ及びネットワークの発達は著しく、文字データ，画像データ，音声データ等，多種の情報がデジタル化され、コンピュータやネットワークを介して扱われるようになってきている。このようなデータはデジタルデータであるために、データの複製が容易にできる環境にある。このため、こうしたデータの著作権を保護するために、デジタル画像データやデジタル音声データの中に著作権情報や利用者情報を電子透かしとして埋め込む処理がなされる場合が多い。
【０００３】この電子透かしとは、デジタル画像データや音声データに所定の処理を施すことによって、これらのデータに密かに情報を埋め込む技術である。この電子透かしをデータから抽出することにより、著作権情報や利用者情報を得ることができ、不正コピーを追跡することが可能である。
【０００４】このような電子透かしを埋め込む方法には、空間領域に埋め込む方式と周波数領域に埋め込む方法の二つに分類できる。このうち、空間領域に埋め込む方式の例としては、パッチワークによるものとしてＩＢＭの方式(W.Bender.D.Gruhl,N.Morimoto,Techniques for Data Hiding,"Proceedings of the SPIE".San Jose CA,USA,February1995)などが挙げられる。また周波数領域に埋め込む方式の例としては、離散コサイン変換を利用するものとしてＮＴＴ方式（中村，小川，高嶋等による“ディジタル画像の著作権保護のための周波数領域における電子透かし方式”，ＳＣＩＳ’９７－２６Ａ，１９９７年１月）の他に、離散フーリエ変換を利用するものとして防衛大の方式（大西，岡，松井，“ＰＮ系列による画像への透かし署名法”，ＳＣＩＳ’９７－２６Ｂ，１９９７年１月）や、離散ウェーブレット変換を利用するものとして三菱，九大の方式（石塚，坂井，櫻井，“ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察”，ＳＣＩＳ’９７－２６Ｄ，１９９７年１月）及び松下方式（“ウェーブレット変換に基づくディジタル・ウォーターマーク画像圧縮，変換処理に対するロバスト性について－”，井上，宮崎，山本，桂，ＳＣＩＳ，９８－３．２．Ａ，１９９８年１月）などが挙げられる。
【０００５】このような電子透かしは、「攻撃」に対して耐性があることが必要である。ここで、電子透かしに対する「攻撃」について簡単に説明する。この「攻撃」とは、透かし情報を消去，或は破壊しようとする行為であり、２通りが考えられる。一つ目は画像処理によるものであり、透かし情報を埋め込んだ画像データに対して、画像圧縮、拡大及び縮小、切り取り、階調変換、プリントアウト及びスキャニングなどの画像処理を施すものを含む。二つ目は人為的なものであり、透かし情報を埋め込んだ画像データに対してノイズを付加することや、透かし情報が埋め込んであると考えられる画像領域を削除することなどを含む。従って、このような攻撃のいずれに対しても、透かし情報は耐性を持つ必要がある。
【０００６】ここで「耐性」とは、埋め込んだ情報が攻撃されても、その埋め込んだ情報を正確に取り出せることが可能であることを意味している。
【０００７】しかしながら、あるアプリケーションでは、画像が攻撃された場合には、埋め込んだ情報を抽出する必要はなく、その代わりに、攻撃された場所などを特定する機能を有することを必要とする場合も考えられる。以下では、この機能のことを「改竄位置検出機能」と呼ぶことにする。
【０００８】従来の、改竄位置検出機能を有する電子透かし方式としては、原画像が１画素当たり複数のビットから構成されるデータである場合には、複数のビットのうちＬＳＢ(Least Significant Bit)のビットを置き換えることにより透かし情報の埋め込みを行い、それを抽出する際には、ＬＳＢのビットだけ読み出すことにより抽出を行っていた。ここで、ＬＳＢとは１画素を構成する複数ビットの情報においてビット位置０（最小位）に位置するビット情報のことで、ビット位置とは、画素を構成するビット系列の中で、そのビットの存在する位置を示すものである。例えば、２^０＝１を表すビットの存在する位置を表す場合、「ビット位置０」と呼び、２^１

＝２（^0は0乗を、^１は１乗を示す）を表すビットの存在する位置を表す場合、「ビット位置１」と呼ぶ。ここで、ビット位置０をＬＳＢと呼ぶのと同様に、１バイトデータにおけるビット位置７をＭＳＢ(Most SignificantBit)と呼ぶことにする。これ以降、「ビット位置」という表現は上述の定義に従うものとする。

【０００９】このようなＬＳＢへの透かし情報の埋め込みによって、画像処理手段を用いた攻撃に対しては、その改竄位置を特定することか可能であった。これは、ＬＳＢが画素を構成するビットのうち最小の大きさを表現しているものであるために、改竄された場合にはＬＳＢのビットは変化しやすく、即ち変化した箇所を改竄された箇所として特定できるからである。ここで正しく抽出できない場合、ＬＳＢが“１”である確率と“０”である確率とが等しくなり、即ち、ランダムに“１”と“０”が出現することが予想される。よって、抽出の結果、ランダムに“１”と“０”が出現している領域を改竄された箇所であると検証することが可能となる。

【００１０】しかしながら、以上のような方式は人為的な攻撃には弱かった。これは、ＬＳＢに固定されて埋め込まれているために、全ての画素のＬＳＢを抽出するといった探索により、電子透かしが埋め込まれたことが第３者に容易に類推されることが考えられる。従って、もし画像データに電子透かしが埋め込まれていることが第三者に知られた場合には、その第三者は透かしが埋め込稀ているＬＳＢの状態をそのままにして、それ以外のビット位置のデータを変更することにより、容易に画像データを容易に改竄することができる。具体例として、画像の内容を改竄する前にＬＳＢの情報を保存しておき、その後、その画像の内容を改竄し、こうして改竄した画像データのＬＳＢだけを予め保存していた情報に置き換えるといった人為的な手段によって、その改竄した画像位置を特定できないようにすることが考えられる。

【００１１】

【発明が解決しようとする課題】以上述べたように従来の技術によれば、透かし情報を埋め込んだ画像に対して改竄を施した場合、その改竄された画像位置を確実に特定することができなかった。

【００１２】本発明は上記従来例に鑑みてなされたもので、データに対して人為的な改竄がなされた場合に、その改竄位置を確実に検出できる画像処理方法及び装置を提供することを目的とする。

【００１３】また本発明の目的は、入力された原画像データの画素位置を指示し、主鍵情報に基づいて、その指示された画素位置の特定の部分を書き換えることにより、入力した画像データに所定のデータを埋め込むことができる画像処理方法及び装置を提供することにある。

【００１４】また本発明の目的は、このような所定のデータが埋め込まれたデータに対してなされた改竄処理を検知し、その改竄位置をも検知できるようにした画像処理方法及び装置を提供することにある。

【００１５】

【課題を解決するための手段】上記目的を達成するために本発明の画像処理装置は以下のような構成を備える。即ち、画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力手段と、主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成手段と、前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更手段と、を有することを特徴とする。

【００１６】また本発明の画像処理装置は、画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力手段と、前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成手段と、前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出手段と、前記抽出手段により抽出された前記画素データと前記鍵情報生成手段により生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較手段とを有し、前記比較手段による比較結果に応じて前記埋め込み済み画像データの改竄位置を検出することを特徴とする。

【００１７】上記目的を達成するために本発明の画像処理方法は以下のような工程を備える。即ち、画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力工程と、主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成工程と、前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更工程と、を有することを特徴とする。

【００１８】また本発明の画像処理方法によれば、画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力工程と、前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成工程と、前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出工程と、前記抽出工程で抽出された前記画素データと前記鍵情報生成工程で生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較工程とを有し、前記比較工程による比較結果に応じて前記埋め込み済み画像データの改竄位置を検出することを特徴とする。

【００１９】

【発明の実施の形態】以下、添付図面を参照して本発明の好適な実施の形態を詳細に説明する。

【００２０】［実施の形態１］図１は、本発明の実施の

形態１に係る電子透かしの埋め込み装置の概略構成を示すブロック図である。

【００２１】図１において、入力部１１へ入力されるデータｘは、１画素当たり所定のビット数を有する多値画像データである。以下では、このデータｘを原画像データと呼ぶ。また入力部１２に入力されるデータｒは、１画素を１ビットで表わす二値画像データで、以下では、このデータを埋め込みデータと呼ぶ。ここで、この埋め込みデータは、人間の視覚にとって意味のある内容であっても、或は人間の視覚にとって意味のない内容であっても良い。意味のある内容である場合には、例えば、著作者の持つロゴマークのようなものであってもよい。この場合は、このロゴマークが埋め込まれた画像から、その著作権情報を読み取ることも可能である。また一方、意味のない内容である場合には、ＩＤの様なものを２進数で表現したものであっても良い。ここでＩＤとは固有の値を意味している。例えば、利用者ＩＤの場合には、その利用者にとって固有の値を表し、デバイスＩＤの場合には、そのデバイスにとって固有の値を表している。この場合、このようなＩＤが埋め込まれた画像から、利用者情報、或は利用デバイス情報などを読み取ることも可能である。

【００２２】また、乱数発生器１３へ入力されるデータＩｖは、乱数発生器１３への初期値、即ち主鍵情報を示している。また、入力部１２へ入力された埋め込みデータｒは、埋め込み画像生成器１４へ入力される。この埋め込み画像生成器１４の詳細な動作については後述する。こうして埋め込み画像生成器１４からは、原画像データｘと等しい面積の画像データが出力され、この画像データはビット置き換え器１５に入力される。また入力部１１へ入力された原画像データｘは、ビット置き換え器１５へ入力される。このビット置き換え器１５の詳細な動作についても後述する。こうして、このビット置き換え器１５からは、原画像データｘのうち埋め込みデータｒにより指定された位置（例えば埋め込みデータｒ’の対応するビットが“１”）の画素情報の特定のビットだけが置き換えられた画像データが出力され、その画像データは出力部１６を介して、埋め込み済み画像データｘ’として出力される。

【００２３】次に、各部の動作の詳細について説明する。

【００２４】まず、埋め込み画像生成器１４の詳細な動作について解説する。

【００２５】埋め込み画像生成器１４は、入力された埋め込みデータｒを基に、その埋め込みデータｒを原画像データｘの大きさに等しいサイズに変換する。以下では、この埋め込み画像生成器１４から出力された画像データを埋め込み画像データｒ’と呼ぶことにする。この埋め込み画像生成器１４におけるサイズ変換には、埋め込みデータｒを繰り返し並べる方式、或は埋め込みデータｒを原画像データｘの大きさに拡大（変倍）処理する方式など、種々のものが考えられる。なお、この埋め込み画像生成器１４から出力される埋め込み画像データｒ’も、１画素に付き１ビットのデータを有する２値データでなければならない。

【００２６】次に、乱数発生器１３の詳細な動作について解説する。

【００２７】乱数発生器１３には、乱数初期値Ｉｖ、即ち主鍵情報が入力される。本実施の形態１に係る処理を安全に用いるために、乱数初期値Ｉｖを公開情報とする場合には、本実施の形態１で用いる乱数発生器１３は、その乱数の発生方式が非公開のもの、或は別の非公開情報を用いるものでなければならない。その一方、乱数発生器１４における乱数発生方式が公開されたものである場合には、乱数初期値Ｉｖを非公開情報としなければならない。つまり、ビット置き換え器１５へ入力される乱数系列、即ち副鍵情報Ｒｎを非公開情報とする必要がある。これらのうち、いずれを公開情報とし、いずれを非公開情報とするかは、各アプリケーションに応じて決定することが可能である。

【００２８】次に、ビット置き換え器１５の詳細な動作について解説する。

【００２９】このビット置き換え器１５は、埋め込み画像データｒ’を原画像データｘに埋め込む、所謂電子透かし埋め込み処理を行う部分である。このビット置き換え器１５においては、埋め込み画像生成器１４から出力された埋め込み画像データｒ’と、入力部１１から出力された原画像データｘの対応する画素位置（例えば埋め込みデータｒ’の対応するビットが“１”）において、その画素値である複数ビット（この実施の形態では８ビット）の内のあるビットの置き換え処理が施される。このビットの置き換え処理は、原画像データｘの持つ輝度値データをビットプレーンに展開した領域に対して施される。いま例えば原画像データが２５６階調（８ビット）を持つ場合、これら８ビットのうちの１ビットが選択されて、このビットが埋め込み画像データｒ’の対応するビットで置き換えられる。この埋め込まれる（選択される）ビット位置は、乱数発生器１３からの出力である副鍵情報Ｒｎによって決定される。

【００３０】例えば、原画像データｘが１画素当たり８ビットの２進符号によって表現されている場合、乱数発生器１３からは“０”から“７”の値を持つ乱数データ列Ｒｎが出力される。この乱数列Ｒｎの値に対応するビット位置が、前述したビット置き換えの対象となるビット位置を示している。

【００３１】ここで、このビット置き換えの対象となるビット位置の選択には、注意が必要である。例えば、選択されるビット位置がＭＳＢに近い値を持つような場合には、埋め込み済み画像データｘ’の画素値が原画像データｘの対応する画素値から大きく異なり、これにより

埋め込み済み画像データｘ’が、原画像データｘに比べて劣化することが予想される。これは、例えば１画素当たり８ビットで構成される画像データの場合に、ＭＳＢの値を変化させることにより、輝度値において２の7乗＝１２８の変化が生じることによる。また、ＬＳＢに限定したビット位置ばかりが選択されると、前述の従来の技術で述べたように、人為的な攻撃に対しては耐性が弱くなる。即ち、例えば、ビット置き換えの対象がＬＳＢ、即ちビット位置０だけに限定されているような場合には、置き換られたビットは容易に書き換えられてしまうと考えられる。また或は、ビット置き換えの対象位置が、ビット位置０とビット位置１である場合には、ビット位置の書き換えには、（ＸＳ×ＹＳ）の2乗の探索を必要とする。ここで、ＸＳ及びＹＳは原画像データｘの横方向の大きさ及び縦方向の大きさを示している。

【００３２】一般に、ビット置き換えの対象位置をビット位置０からビット位置ｎとした場合には、ビット位置の書き換えには、（ＸＳ×ＹＳ）のn乗の探索を必要とする。従って、以上述べたような探索により、埋め込んだ情報（即ち、埋め込んだ全ての画素でのビット位置）が解ってしまった場合、画像の内容を変化させるような改竄が行われた後で、これらの埋め込んだ情報を元の埋め込んだ情報に置き換えることにより、後に述べるビット抽出器２３において、改竄されていない画像であると偽ることが可能となってしまう。この点から、ビット置き換えの対象に選択するビット位置はＬＳＢに近いビット位置が良いといえる。このようにＬＳＢに近いビットを選択して、埋め込みデータｒ’を埋め込むことによって、原画像データｘからの視覚的な画質劣化を抑えて、且つ、画像処理による改竄をされた場合に、その改竄を検証し、更に改竄された位置を特定することが可能となる。即ち、画像が改竄されたにも関わらず、その改竄を検証できなかったり、改竄位置を特定できなくなることが防止できる。

【００３３】以上述べたような処理によって、電子透かしの埋め込み処理を行うことにより、生成された埋め込み済み画像データｘ’は出力部１６を介して出力される。

【００３４】図２は、本発明の実施の形態１に係る電子透かしの抽出装置の概略構成を示すブロック図である。

【００３５】図２において、入力部２１へ入力されるデータｘ’は、前述の図１における電子透かし埋め込み装置から出力された電子透かしの埋め込み済み画像データｘ’である。また乱数発生器２２へ入力されるデータＩｖは、乱数発生器２２への初期値、即ち主鍵情報である。主鍵情報Ｉｖの値は、図１において乱数発生器１３へ入力されるデータＩｖと完全に等しいものでなければならない。

【００３６】入力部２１に入力された埋め込み済み画像データｘ’は、ビット抽出器２３へ入力される。乱数初期値Ｉｖ（主鍵情報）が入力された乱数発生器２２は乱数列（副鍵情報）Ｒｎを生成し、その生成された乱数列ＲｎがビットＲ抽出器２３へ入力される。ビット抽出器２３では、この乱数列Ｒｎを用いて埋め込み済み画像データｘ’からビット情報を抽出する。ここで、乱数発生器２２から出力される乱数列Ｒｎは、前述の図１における乱数発生器１３と同じ構成であるため、ビット抽出器２３が対象とするビット位置も、図１におけるビット置き換え器１５が対象としたビット位置に一致している。よって、以上の処理によって抽出されるビット情報、即ちビット抽出結果を示す画像データｘ’’は、埋め込み済み画像データｘ’が改竄されていない場合には、図１における、原画像データｘに等しいはずである。

【００３７】一方で、埋め込み済み画像データｘ’が改竄されている場合には、埋め込みデータｒとは、改竄されている位置に関して誤って検出される。ここで、埋め込み済み画像データｘ’から検出されたビット抽出結果に対応する画像が正しいか、或は誤っているかの判断は、図１において埋め込みデータｒとしてどのようなものが埋め込まれているかによって方法が違う。

【００３８】例えば、埋め込みデータｒとして、人間の視覚にとって意味のある内容のものが埋め込まれている場合には、図２における改竄位置検出器２４を用いなくても（経路Ａ）人間の視覚によって判断可能である。誤って検出される場合、どのような改竄が行われたかにもよるが、確率的には２進符号“１”と“０”が等しい確率で出現することが予想される。即ち、改竄された箇所は、人間の目には、白色ノイズに近い性質を持つ画像として見えるはずである。

【００３９】更に、図２において埋め込みデータｒが、ビット抽出器２３に入力可能である場合には、この埋め込みデータｒを改竄位置検出器２４に入力することにより、上述の判断は改竄位置検出器２４により行うことが可能である。これは、図２において、改竄位置検出器２４を通る経路、即ちＢの経路を通る場合である。

【００４０】ここで改竄位置検出器２４には、埋め込みデータｒ、及び図２から出力されたビット抽出結果を示す画像データ（Ｂ）が入力される。埋め込みデータｒは、埋め込み画像生成器２６で所定の処理が施された後に、改竄位置検出器２４に入力される。この画像生成器２６で施される処理は、図１における埋め込み画像生成器１４で行われた処理と同様の処理でなければならない。こうして改竄位置検出器２４では、入力された２つの画像データの同じ座標位置においてビットを比較し、等しい場合に“１”を、等しくない場合には“０”を出力する。これにより、ビット抽出結果画像として改竄位置では“０”が、一方で改竄されていない位置では“１”が出力される。このビット抽出結果を示す画像データｃは、アプリケーションが改竄位置を特定するためにも用いることが可能であるし、更に、人間の目によっ

て改竄位置を特定することも可能である。

【００４１】尚、人間の目によって改竄位置を特定する場合には、前述の方式よりも、この方式のほうが正確に微小な改竄を検出することが可能である。

【００４２】更に、埋め込みデータｒが白色単色である場合には、改竄が検出された画素に関しては黒色画素とすることにより、より分かりやすく改竄位置を表現することも可能である。

【００４３】［実施の形態２］次に本発明の実施の形態２について説明する。この実施の形態２では、圧縮された画像データに対して前述の実施の形態１を適用するものである。前述の実施の形態１では、埋め込みの対象となる入力画像データは、１画素当たり所定のビット数（前述の例では８ビット）を持つ多値画像データであった。これに対し本実施の形態２では、埋め込みの対象となる入力画像データは、符号化された画像データである。なお、この符号化された画像データには、ＪＰＥＧによって圧縮された画像データも含まれる。以下、本実施の形態２では、符号化データがＪＰＥＧデータである場合について説明する。

【００４４】まず、ＪＰＥＧ符号化について解説をする。

【００４５】図３（ａ）は、ＪＰＥＧの符号化手順例を説明するブロック図である。

【００４６】まず、符号化する静止画の画像データを８×８画素のブロックに分割し、各ブロック毎にＤＣＴ（離散的コサイン変換）を行う（画像変換器３０１）。以下、そのＤＣＴ（Discreate Cosine Transform）したブロックをＤＣＴ係数ブロック、ＤＣＴ係数ブロックの１係数をＤＣＴ係数、１枚の画像のＤＣＴ係数ブロックの集合をＤＣＴ係数ブロック群と呼ぶとする。

【００４７】次に、ＤＣＴ係数ブロック群を任意の量子化テーブルを用いて、量子化器３０２により量子化を行う。以下、このＤＣＴ係数ブロックを量子化したブロックを量子化ＤＣＴ係数ブロック、１枚の画像の量子化ＤＣＴ係数ブロックの集合を量子化ＤＣＴ係数ブロック群と呼ぶとする。

【００４８】そして、量子化ＤＣＴ係数ブロック群をハフマン符号化する（エントロピー符号化器３０３）。このハフマン符号化したデータがＪＰＥＧデータになる。このとき用いるハフマンテーブルは、予め用意していたテーブルであっても、各画像毎に作成したテーブルであってもよい。

【００４９】ＪＰＥＧデータは、このハフマン符号化したデータと、圧縮時に用いた量子化テーブルとハフマンテーブルを含む（後述：図４参照）。ここで、量子化ＤＣＴ係数ブロックは、各ＤＣＴ係数ブロックを各々量子化テーブルによって定められた値で除算することによって得られる。例えば、輝度成分に対する量子化テーブル、或は色差成分に対する量子化テーブルは、８×８のＤＣＴ係数ブロックに対して、それぞれ図５（ａ）（ｂ）のように与えられる。

【００５０】これらの量子化テーブルは低周波成分により多くのビットを割り当て、高周波成分にはより少ないビットを割り当てるようにして、人間の視覚特性を考慮して構成されている。よって、ＤＣＴ係数ブロックの値が「－３６」である場合、量子化テーブル値が「１８」であればその量子化ＤＣＴ係数ブロック値は「－２」であり、「９９」であればその量子化ＤＣＴ係数ブロック値は「０」である。

【００５１】また、ハフマン符号化は、量子化ＤＣＴ係数をＤＣ係数とＡＣ係数に分けて別々に行われる。ＤＣ係数は１つ前のブロック群のＤＣ係数との差分をＤＣ用のテーブルを用いて符号化される。

【００５２】ＡＣ係数は図６のようなジグザグスキャン順に並び替えて、「０」の係数の連続長（ラン長）と、「０」以外の係数値を組み合わせたテーブルを用いて符号化される。

【００５３】次に、このＪＰＥＧデータの例を図４に示す。

【００５４】図４は、ＪＰＥＧのシーケンシャル方式で圧縮したデータの構成例を示す図である。

【００５５】このシーケンシャル方式とは、デーコードを行うと上から順に鮮明な画像がでてくる方式で、これに対して、最初画像全体を不鮮明に表示し、徐々に鮮明になってくる方式はプログレッシブ方式と呼ばれている。このＪＰＥＧデータは、マーカと呼ばれるデータ内でユニークな２バイトのコードによってフォーマットされている。

【００５６】まず最初の「ＳＯＩ」マーカは、ＪＰＥＧデータのスタートを表わしている。次の「ＤＱＴ」マーカ部は、量子化テーブルの定義を表わしており、圧縮時に使用した量子化テーブルを「ＤＱＴ」マーカの後ろに格納している。次の「ＳＯＦＯ」マーカ部は、ＤＣＴを使ったシーケンシャル方式で圧縮した場合に、「ＳＯＦＯ」マーカを使用し、このマーカの後ろに、圧縮してある画像のサイズやサンプリング率、コンポーネント数、コンポーネント毎の量子化テーブルの識別子等の圧縮時のパラメータが格納される。次の「ＤＨＴ」マーカ部は、ハフマンテーブルの定義を表わしており、この「ＤＨＴ」マーカの後ろには、圧縮時に使用したハフマンテーブルが格納されている。次の「ＳＯＳ」マーカ部は、実際に画像を符号化したハフマン符号を格納している。ここでのハフマン符号は、ＤＣＴ係数の直流成分、及び交流成分において異なる符号化が施されていることに注意する必要がある。

【００５７】ＪＰＥＧにおいては、ＤＣＴ係数のうちの直流成分は、隣り合うＤＣＴブロックの直流成分の差分値をハフマン符号で表現している。一方、交流成分では、差分値は用いず、ブロック内でジグザグスキャンさ

れたシーケンスの零ランレングスと有効係数との組合せをハフマン符号で表現している。このハフマン符号と、有効係数の大きさを最小のビット数で表現した符号の組合せが符号化データである。以降の説明では、前者に相当する符号を「ＧＣ」、後者に相当する符号を「ＶＣ」と定義する。ここで有効係数とは零でない係数である。

【００５８】交流成分のハフマン符号化に関して例を挙げて説明する。

【００５９】例えば、交流成分として直流成分のすぐ右に位置する値「－３」を持つ係数をハフマン符号化する場合を考える。この場合、図７に示すような表を用いて係数がグループ化される。即ち、例えば値「－３」の場合には、グループ番号として「２」が選択される。更に、零ランレングスは「０」である。これらグループ番号と零ランレングスの組合せ（０，２）を基に、図８に示すハフマンテーブルを用いてハフマン符号化される。

【００６０】この例の場合には、「ＧＣ」としてハフマン符号「０１」が選択され記憶される。この後に、「ＶＣ」として「－３」を最小のビット数で表現した「００」が続いて記憶される。その結果として、この例における交流成分「－３」には、「０１００」というハフマン符号が選択される。

【００６１】そして「ＳＯＳ」マーカの後に、コンポーネント毎のハフマンテーブルへの識別子等の情報が入ったヘッダが数バイト続いた後、画像を符号化したハフマン符号が続く。そして最後に、「ＥＯＩ」マーカにより符号化された画像データの終了が示されている。

【００６２】この例ではマーカの順を図４のように示したが、実際のデータではこの順番である必要はないし、またマーカの数が２つ以上の場合もある。

【００６３】図３（ｂ）は、図３（ａ）の手順で圧縮したＪＰＥＧデータの復号化装置の構成例を示したブロック図である。

【００６４】この復号化処理では、まずＪＰＥＧデータ内のハフマンテーブルを用いて、ハフマン符号のハフマン復号化を行って、量子化ＤＣＴ係数ブロック群に復号する（エントロピー復号器３０４）。次に逆量子化器３０５を用いて、量子化ＤＣＴ係数ブロック群を、ＪＰＥＧデータの量子化テーブルを用いて逆量子化し、ＤＣＴ係数ブロック群に復号する。そして次に画像逆変換器３０６により、そのブロック群をＩＤＣＴ（Inverse DCT：逆ＤＣＴ）を行って、８×８画素のブロックに戻し、それを再構成する。このような手順によってＪＰＥＧデータから復号した画像データを得ることができる。

【００６５】図９は、本発明の実施の形態２に係る電子透かし埋め込み装置の概略構成を示すブロック図である。

【００６６】図９において、入力部９０１を介して入力される入力データ(Code)は、図４のようなデータ形式で構成されたＪＰＥＧ符号化データである。また、乱数初期値Ｉｖ、及び乱数発生器９０５は、前述の実施の形態１の乱数発生器１３と同様のものを用いる。入力されたＪＰＥＧ符号化データ(Code)は、解析器９０２において、ＪＰＥＧの符号化フォーマットに従って解析される。ここで解析とは、入力されたビット系列が、ＪＰＥＧの符号化フォーマットに従って、符号化データとして意味のあるデータとして理解されることである。このうち、電子透かしの埋め込みの対象となる交流成分のハフマン符号が、ＤＣＴブロック毎に置換器９０３に入力される。この置換器９０３は、ＤＣＴブロック毎に埋め込みデータｒのビット情報に応じたハフマン符号の置き換えを行う。ここで、ハフマン符号の置き換えの対象となる符号は、できる限りブロックの中で交流成分が望ましい。

【００６７】これは置換器９０２に入力されたスキャンデータの中で、出来るだけ後ろに位置する符号を対象とすることを意味する。なぜなら、スキャンデータはＤＣＴブロックの中でジグザグスキャンされているため、スキャンデータの中で後ろに位置するデータほど高域成分であるからである。

【００６８】次に、選択された符号に対して置き換え処理を行う方式に関して説明する。

【００６９】まず、「ＧＣ」が置き換えの対象となる場合を考える（方式１）。

【００７０】これは前述したように、零ランレングスと有効係数の組合せによって表現されているものである。このため、ハフマン符号の置き換えの結果、零ランレングスの値が変化してしまうような場合には、復号時に正しい復号をすることができない。なぜなら、有効係数の位置を正しく決定することが出来ないからである。これを解決する一つの方式として、ＪＰＥＧ符号化の際に、図８に示すようなハフマンテーブルを用いているような場合には、この表の横方向の置き換えに限定することが考えられる。例えば、符号「００」を符号「０１」に置き換えることなどが考えられる。更に、横方向の置き換えを行った後においては、その後に続く「ＶＣ」の変更が必要である。これは、符号「００」を符号「０１」に置き換えることによって、零ランレングスは変わらないが、その一方で、グループ番号が変わるからである。これに関しては、置き換える前の符号の表現している値との差が最小になるような値を表現する符号を、置き換え後のグループから選択することよって解決可能である。

【００７１】本実施の形態における横方向の置き換えに関しては、例えば、埋め込みデータｒのビット情報が“０”である場合には、最も近い奇数グループ番号へ、一方で埋め込みデータｒのビットが“１”である場合には、最も近い偶数グループ番号へ置き換えることが、画質劣化を最小に抑えるという観点から現実的である。

【００７２】次に、「ＶＣ」が置き換えの対象となる場合を考える（方式２）。

【００７３】これは前述したように、有効係数を最小のビット数で表現しているものである。よって「ＶＣ」の場合のように零ランレングスに関しては関連しない。この符号の置き換えに関しては、ビット数が変化しないような方法であれば、任意の方法が選択可能である。なぜなら、ビット数が変化しないような変化であれば、グループ番号は変わることがなく、即ち正しく復号可能であるからである。実際の置き換えに関しては、その符号のあるビット位置のビットを、埋め込み原画像のビットに置き換えることが考えられる。この時のビット位置は乱数によって選択可能である。

【００７４】以上、述べた方式によってビット置き換えが行われ、出力部９０４を介して、ＪＰＥＧデータが出力される。

【００７５】図１０は、本実施の形態２に係る電子透かしの抽出装置の概略構成を示すブロック図である。

【００７６】図１０において、入力部１００１を介して入力される入力データｘは、図９に示した電子透かし埋め込み装置により、電子透かしが埋め込まれたＪＰＥＧ符号化データｘである。また、乱数初期値Ｉｖ及び乱数発生器９０５に関しては、前述の実施の形態１で説明した乱数発生器１３と同じものである。ここで、入力されたＪＰＥＧ符号化データｘは、解析器１００２において、ＪＰＥＧの符号化フォーマットに従って解析される。このうち、電子透かしが埋め込まれている交流成分のハフマン符号が、ＤＣＴブロック毎に抽出器１００３に入力される。

【００７７】この抽出器１００３は、ＤＣＴブロック毎に符号化データｘから電子透かしを抽出する。この抽出器１００３は、乱数発生器９０５から得られる乱数列Ｒｎによって、ブロック中において、どの符号化された係数に対して電子透かしが埋め込まれているかを特定する。次に、この特定された係数を表現している符号から、電子透かしを抽出する。

【００７８】「ＶＣ」及び「ＧＣ」の両方が置き換えの対象となる場合を考える（方式１に対応）。

【００７９】これは、前述したように、「ＶＣ」と「ＧＣ」の両方に対して、電子透かしの埋め込みが行われており、その符号が属するグループ番号の奇数／偶数によって、ビットを判定することが可能である。

【００８０】入力されたＪＰＥＧデータの中で、「ＨＤＴ」マーカの後に記憶されているハフマンテーブルを用いて、選択されたハフマン符号からグループ番号を求め、これが偶数であった場合ビット“１”を出力し、奇数であった場合ビット“０”を出力する。

【００８１】次に、「ＶＣ」が置き換えの対象となる場合を考える（「方式２」に対応）。これは、選択された符号の中で、乱数Ｒｎにより埋め込みビット位置を特定し、その特定されたビット位置のビット情報を出力することによって抽出可能である。以上の処理により、電子透かしを抽出し、出力部１００４を介して、ビット抽出結果を示す画像として出力される。

【００８２】このビット抽出結果画像から、改竄されているかどうかを検証する方式に関しては、前述の実施の形態１で説明したのと同様の方法を用いることが可能である。

【００８３】［実施の形態３］次に本発明の実施の形態３について説明する。この実施の形態３は実施の形態１或は実施の形態２を、ハッシュ値との組合せによって実現する方式である。

【００８４】一般的に、このハッシュ値を用いることによりディジタルデータが改竄されているかどうかを検証することができる。

【００８５】次に、このハッシュ値について解説する。

【００８６】ハッシュ値ｈとは、ハッシュ関数ｆ：ｘ→ｈにより求められる長い入力例ｘの圧縮値である短い出力ｈである。また、ハッシュ関数ｆは一方向性関数であり、ｒ（ｘ’）＝ｒ（ｘ）を満たす異なる入力ｘ，ｘ’を求めるのは難しいという性質をもつ。このハッシュ関数ｆの代表的なものとしては、ＭＤ５(Message Digest 5)、ＳＨＡ(Secure Hash Algorithm)などがある。このハッシュ関数の詳細については、岡本英司著「暗号理論入門」（共立出版株式会社）に詳しい。

【００８７】以上、述べたような性質を持つハッシュ値を用いて、ディジタルデータの改竄検証を行うことが可能である。

【００８８】これは、あるディジタルデータのハッシュ値ｈがわかっている場合に、そのデータが改竄されているかどうかを検証するためには、改めてディジタルデータのハッシュ値ｈを算出し、それとわかっているハッシュ値ｈと比較することによって実現可能である。即ち、改竄されていない場合は、これらは一致し、改竄されている場合にはこれらは一致しない。

【００８９】以上述べた方式によって、ディジタルデータが改竄されているかどうかを検証することが可能である。しかし、この方式に用いるディジタルデータとして画像データが用いられる場合、あるアプリケーションにおいては、改竄されていた場合には、画像データのどの箇所が改竄されているかを知りたい場合も考えられる。こうした場合、前述の方式では不十分である。なぜなら、ハッシュ値ｈを算出し、比較するといった前述の方式では、画像データの少なくとも１ビットが改竄されている場合には、ハッシュ値ｈが一致しないという比較結果は得られることができるが、その一方で「どこの１ビットが改竄されたか」ということに関しては何ら情報を得る手段がない。

【００９０】そこで、本実施の形態３においては、ハッシュ値ｈによる改竄検出と、前述の実施の形態１或は実施の形態２による改竄検出とを組み合わせる方式を提案する。

【００９１】図１１は、本発明の実施の形態３に係る電子透かしの埋め込み装置の構成を示すブロック図である。

【００９２】本装置への入力は、原データとして、１画素当たり所定数のビットを有する多値画像データ或は符号化データｘ、及び埋め込みデータｒ、及び乱数初期値ｋである。ここで、入力データｘが１画素当たり所定数のビットを持つ多値画像データの場合は、図１１の電子透かし埋め込み器１１０１は、前述の実施の形態１で説明したような方式の装置を用いるべきであり、一方、入力データｘが符号化データの場合には、図１１の電子透かし埋め込み器１１０１は、前述の実施の形態２で説明した方式の装置を用いるべきである。

【００９３】また、埋め込みデータｒ及び乱数初期値ｋは、前述の実施の形態１及び実施の形態２で述べたものと同様のものが考えられる。

【００９４】以上述べた様な構成によって、入力されたデータｘには、電子透かし埋め込み器１１０１によって埋め込みデータｒが埋め込まれる。ここで、電子透かし埋め込み器１１０１から出力されるデータを埋め込み済みデータｘ1と呼ぶ。この埋め込み済みデータｘ1は、演算器１１０２及び合成器１１０３に入力される。演算器１１０２では、この埋め込み済みデータｘ1に対して前述したハッシュ演算などを施し、その演算結果であるハッシュ値ｈなどが出力される。また合成器１１０３には、電子透かし埋め込み器１１０１からの出力である埋め込み済みデータｘ1及び演算器１１０２からの出力である埋め込み済みデータｘ1のハッシュ値ｈが入力され、これらが合成される。この合成には、ハッシュ値ｈを、入力データｘの形式に対応した付加的な情報が記述可能な箇所へ書き込むことなどが考えられる。例えば、入力データｘがＪＰＥＧ符号化データである場合には、その埋め込み済みデータｘ1もＪＰＥＧ符号化データとなる。この場合には、ＪＰＥＧ符号において、ＣＯＭがコメントのためのマーカとして定義されているために、M_COMの後にハッシュ値ｈを記述することが可能である。

【００９５】また同様に、入力データｘが１画素当たり所定数のビットを持つ多値画像データである場合にも、それが用いている画像フォーマットにおいて、付加的な情報を記述可能な箇所へ書き込むことが考えられる。例えば、入力データｘがＰＢＭフォーマットである場合、記号「#」の後に続く改行コードまでのデータは、コメントであるとみなされるため、この領域にハッシュ値ｈを記載することができる。

【００９６】更に、入力データｘがFlashPixファイル・フォーマットの場合では、ハッシュ値ｈを属性情報としてプロパティセットの中に格納しておくこともできる。

【００９７】以上のように、合成器１１０３からはハッシュ値ｈと埋め込み済みデータｘ1とが合成されたデータｘ’が出力される。

【００９８】以下では、この合成器１１０３からの出力をハッシュ値ｈを含む埋め込み済みデータｘ’と呼ぶ。

【００９９】次に図１２は、本実施の形態３に係る改竄検出装置の構成を示すブロック図である。

【０１００】本装置への入力は、図１１に示した電子透かし埋め込み装置から出力されたハッシュ値ｈを含む埋め込み済みデータｘ’及び乱数初期値ｋである。この乱数初期値ｋは、図１１に示す装置において入力されたものと等しい値である場合、正常に電子透かしを抽出することが可能である。この入力されたハッシュ値ｈを含む埋め込み済みデータｘ’は解析器１２０１へ入力される。この解析器１２０１では、入力された画像フォーマットに応じた解析が行われ、ハッシュ値ｈと埋め込み済みデータｘ1を出力する。このうち埋め込み済みデータｘ1は、演算器１２０２及び切替え器１２０４に入力される。演算器１２０２では、図１１の演算器１２０２と同様の演算を実行し、その出力として埋め込み済みデータｘ1のハッシュ値ｈ’が出力される。こうして演算器１２０２からの出力である埋め込み済みデータｘ1のハッシュ値ｈ’と、解析器１２０１から出力されたハッシュ値ｈとが比較器１２０３に入力される。そして、この比較器１２０３において、入力された二つのハッシュ値が等しいかどうかを比較し、その比較結果ｙを出力する。例えば、二つのハッシュ値が等しい場合には制御信号ｙ＝“０”、二つの値が等しくない場合には制御信号ｙ＝“１”を出力する。この制御信号ｙにより、図１２の装置に入力されたデータｘ’が改竄されているかどうかを検証することができる。

【０１０１】更に、比較器１２０３から出力された制御信号ｙは、切替え器１２０４へ入力されても良い。この切替え器１２０４では、解析器１２０１から出力された埋め込み済みデータｘ1を電子透かし抽出器１２０５へ入力し、処理を続行するかどうかを決定する。即ち、この切替え器１２０４は、比較器１２０３から出力された制御信号ｙが“１”である場合には、埋め込み済みデータｘ1を電子透かし抽出器１２０５に入力させ、制御信号ｙが“０”である場合（一致する場合）には、埋め込み済みデータｘ1を電子透かし抽出器１２０５へ入力させずに処理を終了するように動作している。

【０１０２】これにより、入力されたデータが改竄されていた場合には、電子透かしの抽出を行い、入力データが改竄されていない場合には、処理を終了することが可能である。

【０１０３】また切替え器１２０４から出力された制御信号ｙが“１”である場合（一致しない場合）、即ち、埋め込み済み画像が改竄されていた場合には、埋め込み済み画像は電子透かし抽出器１２０５に入力される。電子透かし抽出器１２０５へ入力された埋め込み済み画像からは、乱数初期値ｋを用いて、埋め込まれている電子

透かしが出力される。この電子透かし抽出器１２０５の動作は、前記実施の形態１及び実施の形態２において述べた動作と同様の動作であり、改竄位置を特定することが可能なビット抽出結果画像が出力される以上述べた処理によって、入力されたデータが改竄されているかどうかを検証し、改竄されている場合には、画像上のどの箇所が改竄されていたかを特定することができる。

【０１０４】本発明は上記実施の形態を実現するための装置及び方法及び実施の形態で説明した方法を組み合わせて行う方法のみに限定されるものではなく、上記システム又は装置内のコンピュータ（ＣＰＵあるいはＭＰＵ）に、上記実施の形態を実現するためのソフトウエアのプログラムコードを供給し、このプログラムコードに従って上記システムあるいは装置のコンピュータが上記各種デバイスを動作させることにより上記実施の形態を実現する場合も本発明の範疇に含まれる。

【０１０５】またこの場合、前記ソフトウエアのプログラムコード自体が上記実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、具体的には上記プログラムコードを格納した記憶媒体は本発明の範疇に含まれる。

【０１０６】この様なプログラムコードを格納する記憶媒体としては、例えばフロッピーディスク，ハードディスク，光ディスク，光磁気ディスク，ＣＤ－ＲＯＭ，磁気テープ，不揮発性のメモリカード，ＲＯＭ等を用いることができる。

【０１０７】また、上記コンピュータが、供給されたプログラムコードのみに従って各種デバイスを制御することにより、上記実施の形態の機能が実現される場合だけではなく、上記プログラムコードがコンピュータ上で稼働しているＯＳ（オペレーティングシステム）、あるいは他のアプリケーションソフト等と共同して上記実施の形態が実現される場合にもかかるプログラムコードは本発明の範疇に含まれる。

【０１０８】更に、この供給されたプログラムコードが、コンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能格納ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上記実施の形態が実現される場合も本発明の範疇に含まれる。

【０１０９】以上説明したように本実施の形態によれば、画像全体に弱く透かし情報を埋め込むことによって、改竄位置検出機能を有することを特徴とする電子透かしの埋め込み方法が可能となる。

【０１１０】

【発明の効果】以上説明したように本発明によれば、データに対して人為的な改竄がなされた場合に、その改竄位置を確実に検出できるという効果がある。

【０１１１】また本発明によれば、入力された原画像データの画素位置を指示し、主鍵情報に基づいて、その指示された画素位置の特定の部分を書き換えることにより、入力した画像データに所定のデータを埋め込むことができる。

【０１１２】また本発明によれば、このような所定のデータが埋め込まれたデータに対してなされた改竄処理を検知し、その改竄位置をも検知できるという効果がある。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係る電子透かし埋め込み装置の概要を説明するブロック図である。

【図２】本実施の形態１に係る電子透かし抽出装置の概要を説明するブロック図である。

【図３】ＪＰＥＧ方式の概要を説明する図である。

【図４】ＪＰＥＧによって符号化されたデータのフォーマットを説明する図である。

【図５】ＪＰＥＧにおいて用いられる量子化テーブルの例を説明する図である。

【図６】ＪＰＥＧにおいて用いられるジグザグスキャンを説明する図である。

【図７】ＪＰＥＧにおいて用いられる交流成分のグループ分けのための例を説明する図である。

【図８】ＪＰＥＧにおいて用いられる交流成分のハフマンテーブルの例を説明する図である。

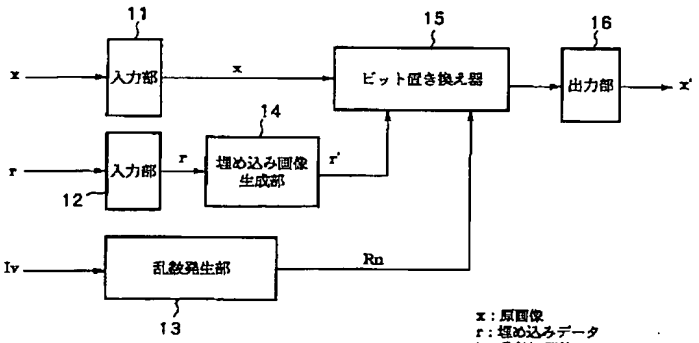
【図９】本発明の実施の形態２に係る電子透かし埋め込み装置の概要を説明するブロック図である。

【図１０】本実施の形態２に係る電子透かし抽出装置の概要を説明するブロック図である。

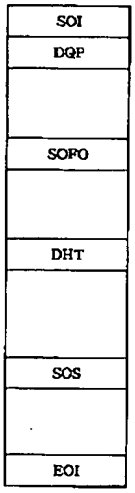
【図１１】本発明の実施の形態３に係る電子透かし埋め込み装置の概要を説明するブロック図である。

【図１２】本実施の形態３に係る電子透かし抽出装置の概要を説明するブロック図である。

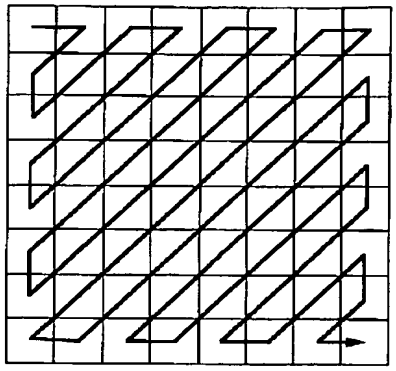
【図１】



【図４】



【図６】



【図５】

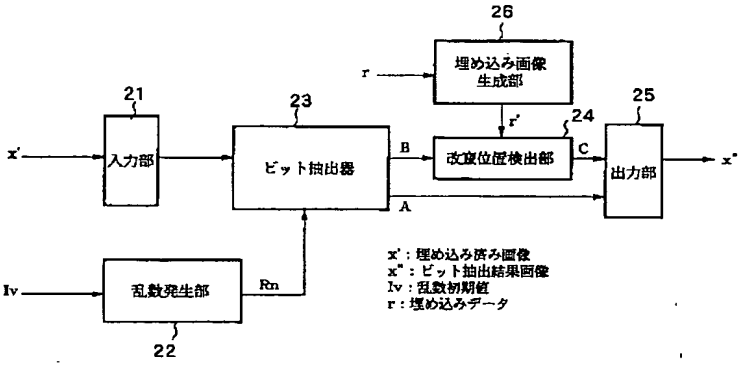
(a)

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

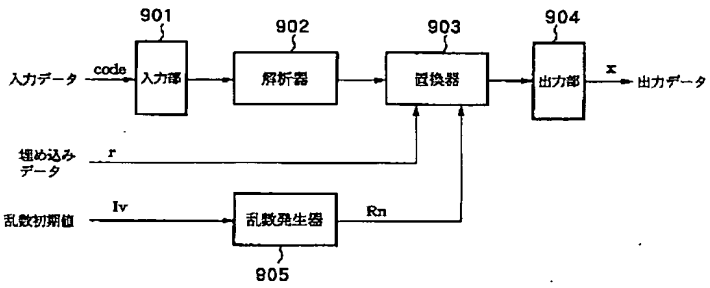
(b)

17	18	24	47	66	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
66	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

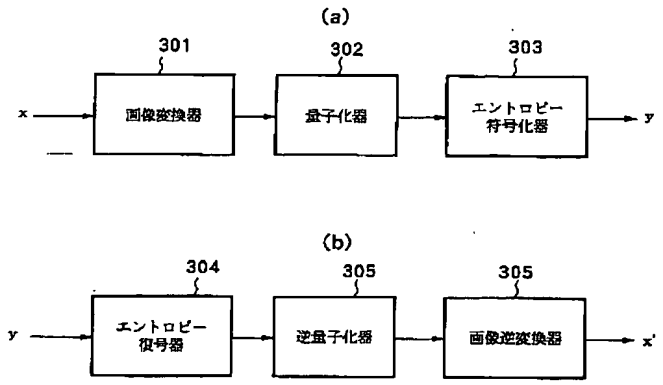
【図２】



【図９】



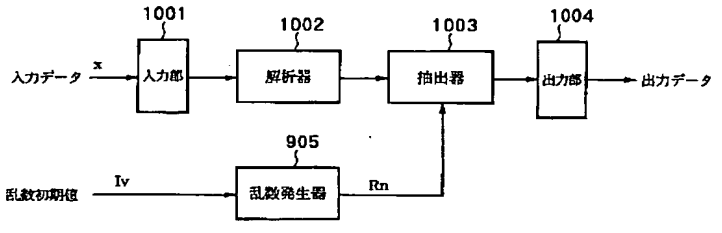
【図３】



【図７】

AC係数	グループ番号	ランク長	
		0	1　2　. . .　14　15
0	0	EOB	. . .
−1,1	1	00	. . .
−3,−2,2,3	2	01	. . .
−7..−4,4..7	3	100	. . .
−15..−8,8..15	4	1011	. . .
−31..−16,16..31	5	11010	. . .
−63..−32,32..63	6	:	
−127..−64,64..127	7	:	
−255..−128,128..255	8	:	
以下省略			

【図１０】

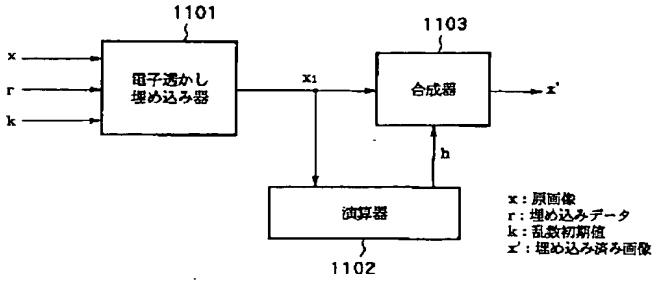


【図８】

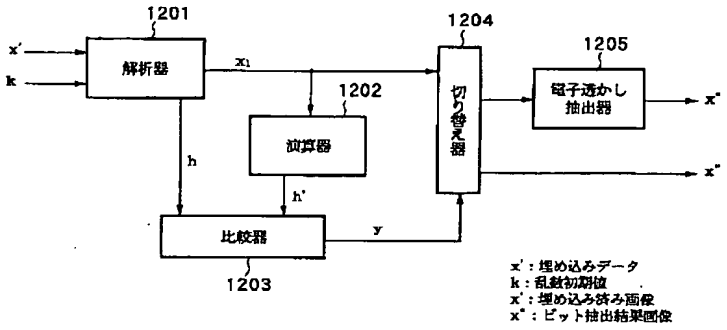
AC係数のグループ番号

零ランレングス	0	1	2	3	...	15
0	EOB	00	01	100		
1						
...						
14						
15	ZRL					

【図１１】



【図１２】



フロントページの続き

Ｆターム(参考)　5B017 AA06 BA05 BA07 BB03 CA08
CA09 CA16
5B057 CA02 CA08 CA12 CA16 CB02
CB06 CB08 CB12 CB16 CB19
CC03 CE08 CE09 CG07 CH08
CH20 DA07 DA17
5C076 AA14 AA40 BA06 CA10

(TRANSLATION)

Docket No. 5037620072 Mailing No. 033180

Mailing Date: February 3, 2004

NOTICE OF REASONS OF REJECTION

Patent Application Number:	2001-025664 for patent
Drafted Date:	January 27, 2004
Examiner:	Keigo SHIRAISHI 9856 5V00
Agent:	Hiroshi MAEDA (and other 7 persons)
Applied Law:	Sections 29(2) and 36

This application is deemed to be rejected for the following reasons. If there is any opinion thereagainst, an Argument should be filed within 60 days from the mailing date of this Notice of Reasons of Rejection.

REASONS

[A]. The inventions according to the below-mentioned Claims of this application are such as could readily be inferred, on the basis of the inventions disclosed in the publications listed below distributed prior to the filing date of this application in Japan and/or foreign countries or the inventions available to public via electric communication lines, by those who have common knowledge in the technical field to which the invention belongs. Hence, under the provision of Patent Law Section 29(2), it cannot be

patented.

REMARKS (see the below citation list about cited references.)

- Claim(s): 1 and 13
- Citation(s): 1
- Comment:

Citation 1 discloses an apparatus for embedding watermark information in image data compressed by DCT, quantization, run length encoding and Huffman coding, comprising a variable length decoding means for extracting a codeword (GC) and an additional bit or bits (VC) (definition paragraph [0057]) corresponding to the codeword from the compressed image data based on a Huffman table; an embedding means (see particularly [0072] to [0073]) for embedding watermark information in a prescribed bit of the additional bits extracted by the variable length decoding means; and a connecting means for connecting the additional bits having the watermark information embedded therein by the embedding means with the codeword extracted by the variable length decoding means to produce a variable length code.

- Claim(s): 2 and 16
- Citation(s): 1
- Comment:

Citation 1 discloses, at [0067], embedding in a high-pass component in a DCT block.

- Claim(s): 3 and 19
- Citation(s): 1
- Comment:

It is a conventional method to embed watermark information in data of which bit length is large.

- Claim(s): 4 and 22
- Citation(s): 1
- Comment:

It is a conventional method to embed watermark information in a prescribed color component.

- Claim(s): 9 to 12 and 28 to 31
- Citation(s): 1
- Comment:

To allow a header to store an area where watermark information is embedded and to extract the watermark information based on this area stored in the header are well known.

- Claim(s): 14, 17, 20 and 23
- Citation(s): 1 and 2
- Comment:

It is a well known technique to interpose electronic watermark in consideration of degradation in quality of image, as disclosed in Citation 2.

・Claim(s): 15, 18 and 21

・Citation(s): 1

・Comment:

It is a matter that a person skilled in the art naturally performs to increase the area where watermark information is to be embedded when there generates lack in this area.

CITATION LIST

1. JP 2001-024876A
2. JP 2000-032406A

[B] This application does not comply with the requirement under Patent Law Section 36(6)(ii) in the following point.

REMARKS

(Omitted)

[C] This application does not comply with the requirement under Patent Law Section 36(6)(i) in the following point.

REMARKS

(Omitted)

At the present, no reason of rejection is found for the inventions drawn to claims other than the above claims specified in the present Notice of

Reasons of Rejection. If any reason of rejection is newly found, it will be notified.

Record of Result of Search for Prior Art References

- Searched Field IPC 7th Edition H04N 1/387
- Prior Art Reference

JP 2000-013764A

JP 2001-007705A

JP 2000-151973A

This Record of Result of Search for Prior Art References does not constitute the reasons of rejections.

拒絶理由通知書

特許出願の番号	特願２００１－０２５６６４
起案日	平成１６年　１月２７日
特許庁審査官	白石　圭吾　９８５６　５Ｖ００
特許出願人代理人	前田　弘（外　７名）　様
適用条文	第２９条第２項、第３６条

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

［Ａ］この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　　（引用文献等については引用文献等一覧参照）

・請求項：１，１３
・引用文献等：１
・備考：
引用文献１には、ＤＣＴ・量子化・ランレングス符号化・ハフマン符号化が施されてすでに圧縮されている画像データに透かし情報を埋め込む装置であって、符号語（ＧＣ）と当該符号語に対応する付加ビット（ＶＣ）（定義段落【００５７】）とをハフマンテーブルに基づいて圧縮画像データから抽出する可変長復号化手段と、前記可変長復号化手段によって抽出された付加ビットの所定のビットに透かし情報を埋め込む埋め込み手段（特に段落【００７２】～【００７３】を参照）と、前記埋め込み手段によって透かし情報が埋め込まれた付加ビットと前記可変長復号化手段によって抽出された符号語とを連結して可変長符号を生成する連結手段とを備える情報埋め込み装置が記載されている。

・請求項：２，１６
・引用文献等：１

・備考：
引用文献１の段落【００６７】には、ＤＣＴブロックの中で、高域成分に埋め込むことが記載されている。

・請求項：３，１９
・引用文献等：１
・備考：
ビット長の長いデータに透かし情報を埋め込むことは常套手段である。

・請求項：４，２２
・引用文献等：１
・備考：
特定の色成分にのみ透かし情報を入れることは常套手段である。

・請求項：９－１２，２８－３１
・引用文献等：１
・備考：
ヘッダに透かし情報の埋め込み場所を格納すること、また、ヘッダに格納された埋め込み場所に基づいて透かし情報を取り出すことは周知技術である。

・請求項：１４，１７，２０，２３
・引用文献等：１，２
・備考：
引用文献２に記載されているように、画像の劣化を考慮して電子透かしを挿入することは周知技術である。

・請求項：１５，１８，２１
・引用文献等：１
・備考：
透かし情報に対して埋め込み場所が不足した場合に埋め込み場所を増やすことは当業者が当然なし得ることである。

引　用　文　献　等　一　覧

１.特開２００１－０２４８７６号公報
２.特開２０００－０３２４０６号公報

［B］この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第２号に規定する要件を満たしていない。

記

請求項５，７，２４，２６には、前処理として符号語の数をカウントすることが記載されているが、当該前処理が他の構成要件（本処理）とどのように関連するのかが明確でない。

［C］この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第１号に規定する要件を満たしていない。

記

請求項６，８，２５，２７には、カウントされた符号語の数に基づいて埋め込み領域を指定する旨が記載されているが、段落【０１７０】では、「カウントされた符号語数および埋め込むべき透かし情報の情報量に基づいて」と記載されている。

よって、請求項６，８，２５，２７に係る発明は、発明の詳細な説明に記載したものでない。

この拒絶理由通知書中で指摘した請求項以外の請求項に係る発明については、現時点では、拒絶の理由を発見しない。拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

先行技術文献調査結果の記録

・調査した分野　　ＩＰＣ第７版　Ｈ０４Ｎ　１／３８７
・先行技術文献
特開２０００－１３７６４号公報
特開２００１－７７０５号公報
特開２０００－１５１９７３号公報
この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。